

What is claimed is:

Sub  
a'

1. An apparatus comprising:  
2       an interface to map a device via a bus to an address space of a chipset in a secure  
3       environment for an isolated execution mode, the secure environment being associated  
4       with an isolated memory area accessible by at least one processor, the at least one  
5       processor operating in one of a normal execution mode and the isolated execution mode;  
6       and  
7       a communication storage corresponding to the address space to allow the device  
8       to exchange security information with the at least one processor in the isolated execution  
9       mode in a remote attestation.

1       2. The apparatus of claim 1 wherein the security information includes at least  
2       one of a static public key and a static key certificate.

1       3. The apparatus of claim 2 wherein the interface comprises:  
2       a decoder to decode the address space onto the bus so that an access to the chipset  
3       is passed to the device.

1       4. The apparatus of claim 3 wherein the device accesses a chipset storage via  
2       the address space.

1       5. The apparatus of claim 4 wherein the communication storage comprises:  
2           a configuration storage to store device configuration information.

1       6. The apparatus of claim 5 wherein the communication storage further  
2           comprises:

3           a status register to store device status of the device;  
4           a command register to store a device command for a command interface set; and  
5           an input/output block (IOB) to store input and output data corresponding to the  
6           command.

1       7. The apparatus of claim 6 wherein the configuration storage comprises:  
2           a public key storage to store the static public key;  
3           a key certificate storage to store the static key certificate; and  
4           an interface set storage to store an interface set identifier, the interface set  
5           identifier identifying a command interface set supported by the device.

1       8. The apparatus of claim 7 wherein the configuration storage further  
2           comprises:

3           a manufacturer identifier storage to store a manufacturer identifier; and  
4           a revision storage to store a revision identifier.

1           9.       The apparatus of claim 7 wherein the command interface set is an  
2       initialization set, the initialization set supporting a reset command and a connect  
3       command.

1           10.      The apparatus of claim 7 wherein the command interface set is an  
2       attestation set, the attestation set performing at least one of a public key enumeration, a  
3       key certificate enumeration, and a signing operation.

1           11.      The apparatus of claim 10 wherein the status register comprises:  
2           a connection field to provide a connection status to indicate that the device is  
3       responsive to the connect command; and  
4           an estimate field to provide an estimate of processing time for an operation  
5       specified in the command.

1           12.      The apparatus of claim 11 wherein the status register further comprises:  
2           a self-test field to indicate status of a self test in response to the reset command.

1        13.    The apparatus of claim 10 wherein the public key enumeration enumerates  
2    an additional public key other than the static public key.

1        14.    The apparatus of claim 10 wherein the key certificate enumeration  
2    enumerates an additional key certificate other than the static key certificate.

1        15.    The apparatus of claim 10 wherein the sign operation generates a signature  
2    to attest validity of the secure environment using a private key provided by the chipset.

1        16.    The apparatus of claim 15 wherein the signature corresponds to signing a  
2    chipset parameter.

1        17.    The apparatus of claim 16 wherein the chipset parameter is one of a  
2    chipset isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

1        18.    The apparatus of claim 17 wherein the chipset isolated nub loader hash  
2    and the chipset isolated hash log are stored in the chipset storage.

1           19. The apparatus of claim 18 wherein the software hash and the nonce are  
2 provided by a process nub.

1           20. The apparatus of claim 19 wherein the output data include the signature.

1           21. A method comprising:

2           mapping a device via a bus to an address space of a chipset in a secure  
3 environment for an isolated execution mode, the secure environment being associated  
4 with an isolated memory area accessible by at least one processor, the at least one  
5 processor operating in one of a normal execution mode and the isolated execution mode;  
6 and

7           exchanging security information between the device and the at least one processor  
8 in the isolated execution mode in a remote attestation via a communication storage  
9 corresponding to the address space.

1           22. The method of claim 21 wherein the security information includes at least  
2 one of a static public key and a static key certificate.

1           23. The method of claim 22 wherein mapping comprises:

2            decoding the address space onto the bus so that an access to the chipset is passed  
3            to the device.

1            24.      The method of claim 23 wherein the device accesses a chipset storage via  
2            the address space.

1            25.      The method of claim 24 wherein exchanging comprises:  
2            storing device configuration information in a configuration storage.

1            26.      The method of claim 25 wherein exchanging further comprises:  
2            storing device status of the device in a status register;  
3            performing a device command corresponding to a command interface set to a  
4            command register; and  
5            storing input and output data corresponding to the command in an input/output  
6            block (IOB).

1            27.      The method of claim 26 wherein storing in the configuration storage  
2            comprises:  
3            storing the static public key in a public key storage;

4           storing the static key certificate in a key certificate storage; and  
5           storing an interface set identifier in an interface set storage, the interface set  
6        identifier identifying a command interface set supported by the device.

1           28.     The method of claim 27 wherein storing in the configuration storage  
2        further comprises:  
3           storing a manufacturer identifier in a manufacturer identifier storage; and  
4           storing a revision identifier in a revision storage.

1           29.     The method of claim 27 wherein performing the device command  
2        comprises performing a reset command and a connect command corresponding to an  
3        initialization set.

1           30.     The method of claim 27 wherein performing the device command  
2        comprises performing at least one of a public key enumeration, a key certificate  
3        enumeration, and a signing operation, the public key enumeration, the key certificate  
4        enumeration, and the signing operation corresponding to an attestation set.

1           31.     The method of claim 30 wherein storing the device status comprises:

2 providing a connection status to indicate that the device is responsive to the  
3 connect command; and

4 providing an estimate of processing time for an operation specified in the  
5 command.

1 32. The method of claim 31 wherein storing the device status further  
2 comprises:

3 indicating status of a self test in response to the reset command.

1 33. The method of claim 30 wherein performing the public key enumeration  
2 comprises enumerating an additional public key other than the static public key.

1 34. The method of claim 30 wherein performing the key certificate  
2 enumeration comprises enumerating an additional key certificate other than the static key  
3 certificate.

1 35. The method of claim 30 wherein performing the sign operation comprises  
2 generating a signature to attest validity of the secure environment using a private key  
3 provided by the chipset.

1           36.   The method of claim 35 wherein the signature corresponds to signing a  
2   chipset parameter.

1           37.   The method of claim 36 wherein the chipset parameter is one of a chipset  
2   isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

1           38.   The method of claim 37 wherein the chipset isolated nub loader hash and  
2   the chipset isolated hash log are stored in the chipset storage.

1           39.   The method of claim 38 wherein the software hash and the nonce are  
2   provided by a process nub.

1           40.   The method of claim 39 wherein the output data include the signature.

1           41.   A computer program product comprising:

2           a machine readable medium having program code embedded therein, the  
3   computer program product comprising:

4 computer readable program code for mapping a device via a bus to an address  
5 space of a chipset in a secure environment for an isolated execution mode, the secure  
6 environment being associated with an isolated memory area accessible by at least one  
7 processor, the at least one processor operating in one of a normal execution mode and the  
8 isolated execution mode; and

9 computer readable program code for exchanging security information between the  
10 device and the at least one processor in the isolated execution mode in a remote  
11 attestation via a communication storage corresponding to the address space.

1 42. The computer program product of claim 41 wherein the security  
2 information includes at least one of a static public key and a static key certificate.

1 43. The computer program product of claim 42 wherein the computer readable  
2 program code for mapping comprises:

3 computer readable program code for decoding the address space onto the bus so  
4 that an access to the chipset is passed to the device.

1 44. The computer program product of claim 43 wherein the device accesses a  
2 chipset storage via the address space.

1        45.    The computer program product of claim 44 wherein the computer readable  
2 program code for exchanging comprises:

3              computer readable program code for storing device configuration information in a  
4 configuration storage.

1        46.    The computer program product of claim 45 wherein the computer readable  
2 program code for exchanging further comprises:

3              computer readable program code for storing device status of the device in a status  
4 register;

5              computer readable program code for performing a device command corresponding  
6 to a command interface set to a command register; and

7              computer readable program code for storing input and output data corresponding  
8 to the command in an input/output block (IOB).

1        47.    The computer program product of claim 46 wherein the computer readable  
2 program code for storing in the configuration storage comprises:

3              computer readable program code for storing the static public key in a public key  
4 storage;

5 computer readable program code for storing the static key certificate in a key  
6 certificate storage; and

7 computer readable program code for storing an interface set identifier in an  
8 interface set storage, the interface set identifier identifying a command interface set  
9 supported by the device.

1 48. The computer program product of claim 47 wherein the computer readable  
2 program code for storing in the configuration storage further comprises:

3 computer readable program code for storing a manufacturer identifier in a  
4 manufacturer identifier storage; and

5 computer readable program code for storing a revision identifier in a revision  
6 storage.

1 49. The computer program product of claim 47 wherein the computer readable  
2 program code for performing the device command comprises performing a reset  
3 command and a connect command corresponding to an initialization set.

1 50. The computer program product of claim 47 wherein the computer readable  
2 program code for performing the device command comprises performing at least one of a  
3 public key enumeration, a key certificate enumeration, and a signing operation, the public  
4 key enumeration, the key certificate enumeration, and the signing operation  
5 corresponding to an attestation set.

1        51.    The computer program product of claim 50 wherein the computer readable  
2 program code for storing the device status comprises:

3              computer readable program code for providing a connection status to indicate that  
4 the device is responsive to the connect command; and

5              computer readable program code for providing an estimate of processing time for  
6 an operation specified in the command.

1        52.    The computer program product of claim 51 wherein the computer readable  
2 program code for storing the device status further comprises:

3              computer readable program code for indicating status of a self test in response to  
4 the reset command.

1        53.    The computer program product of claim 50 wherein the computer readable  
2 program code for performing the public key enumeration comprises enumerating an  
3 additional public key other than the static public key.

1        54.    The computer program product of claim 50 wherein the computer readable  
2 program code for performing the key certificate enumeration comprises enumerating an  
3 additional key certificate other than the static key certificate.

1        55.    The computer program product of claim 50 wherein the computer readable  
2 program code for performing the sign operation comprises generating a signature to attest  
3 validity of the secure environment using a private key provided by the chipset.

1        56.    The computer program product of claim 55 wherein the signature  
2 corresponds to signing a chipset parameter.

1        57.    The computer program product of claim 56 wherein the chipset parameter  
2 is one of a chipset isolated nub loader hash, a chipset isolated hash log, a software hash,  
3 and a nonce.

1        58.    The computer program product of claim 57 wherein the chipset isolated  
2 nub loader hash and the chipset isolated hash log are stored in the chipset storage.

1        59.    The computer program product of claim 58 wherein the software hash and  
2 the nonce are provided by a process nub.

1        60.    The computer program product of claim 59 wherein the output data  
2 include the signature.

1           61. A system comprising:

2           at least one processor operating in a secure environment, the at least one processor  
3           having one of a normal execution mode and an isolated execution mode;

4           a memory coupled to the at least one processor, the memory having an isolated  
5           memory area accessible to the at least one processor in the isolated execution mode; and

6           a chipset coupled to the at least one processor and the memory, the chipset having  
7           a circuit, the circuit comprising:

8           an interface to map a device via a bus to an address space of the chipset in  
9           the secure environment, and

10          a communication storage corresponding to the address space to allow the  
11           device to exchange security information with the at least one processor in  
12           the isolated execution mode in a remote attestation.

1           62. The system of claim 61 wherein the security information includes at least  
2           one of a static public key and a static key certificate.

1           63. The system of claim 62 wherein the interface comprises:

2           a decoder to decode the address space onto the bus so that an access to the chipset  
3           is passed to the device.

1       64.   The system of claim 63 wherein the device accesses a chipset storage via  
2   the address space.

1       65.   The system of claim 64 wherein the communication storage comprises:  
2   a configuration storage to store device configuration information.

1       66.   The system of claim 65 wherein the communication storage further  
2   comprises:  
3       a status register to store device status of the device;  
4       a command register to store a device command for a command interface set; and  
5       an input/output block (IOB) to store input and output data corresponding to the  
6   command.

1       67.   The system of claim 66 wherein the configuration storage comprises:  
2       a public key storage to store the static public key;  
3       a key certificate storage to store the static key certificate; and  
4       an interface set storage to store an interface set identifier, the interface set  
5   identifier identifying a command interface set supported by the device.

1           68.   The system of claim 67 wherein the configuration storage further  
2 comprises:

3           a manufacturer identifier storage to store a manufacturer identifier; and  
4           a revision storage to store a revision identifier.

1           69.   The system of claim 67 wherein the command interface set is an  
2 initialization set, the initialization set supporting a reset command and a connect  
3 command.

1           70.   The system of claim 67 wherein the command interface set is an  
2 attestation set, the attestation set performing at least one of a public key enumeration, a  
3 key certificate enumeration, and a signing operation.

1           71.   The system of claim 70 wherein the status register comprises:  
2           a connection field to provide a connection status to indicate that the device is  
3 responsive to the connect command; and  
4           an estimate field to provide an estimate of processing time for an operation  
5 specified in the command.

1        72.     The system of claim 71 wherein the status register further comprises:  
2              a self-test field to indicate status of a self test in response to the reset command.

1        73.     The system of claim 70 wherein the public key enumeration enumerates an  
2              additional public key other than the static public key.

1        74.     The system of claim 70 wherein the key certificate enumeration  
2              enumerates an additional key certificate other than the static key certificate.

1        75.     The system of claim 70 wherein the sign operation generates a signature to  
2              attest validity of the secure environment using a private key provided by the chipset.

1        76.     The system of claim 75 wherein the signature corresponds to signing a  
2              chipset parameter.

1        77.     The system of claim 76 wherein the chipset parameter is one of a chipset  
2              isolated nub loader hash, a chipset isolated hash log, a software hash, and a nonce.

1           78.   The system of claim 77 wherein the chipset isolated nub loader hash and  
2   the chipset isolated hash log are stored in the chipset storage.

1           79.   The system of claim 78 wherein the software hash and the nonce are  
2   provided by a process nub.

1           80.   The system of claim 79 wherein the output data include the signature.